WORK STUDY

DIGITAL SURVEILLANCE IN SERBIA

Andrijana Ristić

BCSP Belgrade Centre for Security Policy

July 2023

DIGITAL SURVEILLANCE IN SERBIA

Publisher:
BBelgrade Centre for Security Policy
Đure Jakšića 6/5 Belgrade
www.bezbednost.org, office@bezbednost.org

Author:
Andrijana Ristić

Translation:
Alisa Radić

Design and pre-press:
Srđan Ilić

July 2023

BCSP Belgrade Centre for Security Policy

Sadržaj

Introduction

People's ever stronger reliance on digital technologies and devices has caused states and private actors to increasingly reach for various systems and tools for digital surveillance of citizens. Consequently, high-resolution cameras, artificial intelligence, programmes for biometric recognition, tools for automatic data collection from the Internet and intrusive software for monitoring mobile phones have become the everyday reality of people around the world. Unfortunately, Serbia is not exempted from this trend. Domestic investigative journalists, as well as renowned foreign research organisations such as Citizens Lab, established that Serbian security institutions have procured numerous digital tools for the surveillance of citizens (including those that are most intrusive and capable of secretly infiltrating and controlling digital devices), as well as high-resolution cameras that can be easily equipped with facial recognition software. However, not only security institutions procured programmes and equipment for digital surveillance; they were also obtained bu those whose jurisdiction does not include national and public security, such as e.g. the public company *Elektroprivreda Srbije* (EPS) [the Electric Power Company of Serbia], the Ministry of Trade, Tourism and Telecommunications, the Market Inspection and the tax police.

The spread of digital surveillance in Serbia is highly non-transparent, and especially dangerous since Serbia has been assessed as a captured state characterised by the abuse of state resources for the sake of personal and party interests. Although the reports by the media and investigative journalists are important, they are focused on individual cases, which makes it difficult to get a broader picture of the scale of the digital surveillance problem in Serbia based on them. That is why it is important, starting from the existing reports, to map the digital surveillance infrastructure in Serbia, i.e. to make a list of digital surveillance equipment and programmes the state institutions have acquired, determine whether they are competent and authorised to use them, and how these technologies are misused. Since Serbia is striving to become a member of the European Union (EU), it is also important to show how the EU is attempting to regulate this area.

Description of Digital Technologies that Threaten the Privacy of Citizens in Serbia

In 2020, the company **Huawei** signed a contract with the Ministry of the Interior on the procurement of several thousand cameras for smart video surveillance. However, what poses a problem is the absence of information about how these cameras actually work and what sort of information they collect. In addition to video surveillance, the **IPC6625-Z30** and **IPC6225-VRZ-ES** mounted cameras can also perform smart video analysis that includes object identification, target color recognition, and vehicle recognition. The former stands out because it has a 30x optical zoom and an infrared lamp that can reach up to 150 metres even in low-light conditions, while the latter has the same features but on a slightly smaller scale.[1]

Attention should also be focused on the **VCN3020** analysis system, which displays data from smart cameras in the central office in real time and has video reproduction capabilities. The analysis results are then kept in the storage system, Ocean Store, and if necessary, further video analysis can be performed using the **VCM5020** analytics system, which, in addition to traditional video analysis methods, also uses biometric technology for facial recognition and human behavior analysis, all for the purpose of identifying the person in the video.[2]

The sophisticated Pegasus tracking programme is a product of another Israeli company, NSO Group. This spyware contains the most advanced technology of its kind, which allows the user to hack a person's telephone remotely, without the victim even noticing. Pegasus can access both the camera and the microphone, as well as any data that is stored in the phone, including messages, calls and emails. The software does not require the victim to click on a suspicious link, but rather infects the attacked system without any interaction. The British newspaper *Guardian* disclosed the Pegasus Project, revealing the presence of this spyware in no less than 50,000 mobile devices, including the telephone of French President Emmanuel Macron. Numerous cases of misuse of this spyware led to its worldwide prohibition. The United States Department of Commerce blacklisted the NSO Group and prohibited trading with this company without a special license, while the American company Apple sued the Group for hacking its users.[3] Many governments – including Greece at the end of 2022[4] – have banned the purchase and possession of this software.

Circles, a company affiliated with the NSO Group, also develops surveillance software that exploits weaknesses in mobile systems to monitor phone calls, messages and phone locations without having to hack the device. Certain states that use these technologies to violate human rights are the clients of this company, and the use of the software by the Royal Thai Army, which is suspected of torturing prisoners who were most likely detained using this software, is directly related.[5]

Cyberbit Solutions is an Israeli company that produces powerful computer hacking and spying spyware that sends a video link to the victim via email; once the victim activates the link, the spyware is installed without his/her knowledge. Once this software is in the computer, it can access all the documents and data on it and continue to monitor and record all future activities. There are several examples of its misuse, but the case where Ethiopia carried out espionage attacks against Oromo dissidents outside the country using this software, as well as against Eritrean companies and government agencies, stands out.[6]

Predator is another spyware similar to Pegasus. It hacks the victim's phone, gaining access to all information on the device such as messages, photographs/images and saved passwords. It also accesses the camera and microphone, through which it spies on the victim and tracks his/her calls. Unlike Pegasus, Predator can only activate its spyware if the victim clicks on a suspicious link. The manufacturer of this software is Cytrox, a company that was founded by Israeli and Hungarian citizens in North Macedonia.[7] Predator is believed to be used by many governments to spy on journalists and the opposition. The danger of such software became known to the public after a case where the Greek government secretly kept sending money to a company that sells this software, and officials admitted to using it to intercept the communication of at least one journalist and a representative of the European Parliament without a court order. These discoveries were followed by numerous resignations at the very top of the Greek government and the increased regulation of similar software.[8]

Fin Spy is a computer and telephone spying programme that exploits security flaws in software updates to "attack" a targeted device, produced by the German conglomerate Fin Fisher. Once installed, the programme collects all data, intercepts calls and tracks the victim's location. Fin Fisher first appeared in Turkey in 2017, where its targets were the activists who participated in anti-government demonstrations. Due to the German government's investigation into the company's operations caused by the illegal sale of spyware to the Turkish government, which is linked to numerous violations of human rights and freedoms, Fin Fisher declared bankruptcy and ceased to operate.[9] Many other companies produce such software and operate in the same way, so there are many similar tools on the market.

Cognyte is an Israeli company that produces espionage software which has the ability to merge, analyse and visualise a large number of different data sets in order to find information and define patterns of behaviour. However, the problem is that this software often uses fake social media accounts to trick victims into providing the required data. Until now, this software has been used mainly to spy on journalists, political opponents and activists. The fact that Facebook blocked the accounts of this company on their platforms indicates the danger of this and similar software.[10] The company has also been accused of using its technology for massive human rights abuses in Myanmar.[11]

Griffeye Analyze, made by the Swedish company Griffeye, is a software for facial recognition and video analysis that compares and connects collected data with other data that are available on the Internet.[12] Although its primary role is to detect and prevent sexual exploitation of children, this powerful software can also be misused for the purpose of the authorities' confrontation with members of opposition or activists at protests, which is not difficult to imagine without a clear legal framework that would limit the use of such technologies.

Hacking Team was an Italian spyware company based in Milan. Of particular interest to security services around the world were its remote control systems, which were based on targeted spread of viruses to computers and telephones by sending infected documents whose downloading triggered the installation of spyware, which would then proceed to further collect data from infected devices. After the company's initial successes, software abuse led a hacktivist known as Phineas Fisher to break into Hacking Team's servers and release 400 gigabytes of sensitive data, which revealed that the company was selling its software to dictatorial regimes known for massive human rights abuses and whose victims were often journalists and activists. The company Hacking Team ceased to exist, that is, another cyber security company purchased it and gace it a new name: Momento Labs.[13]

Trovicor is an interception and intelligence technology company. It possesses equipment for legal interception through specialised monitoring centres that can intercept telephone calls, SMS messages and all Internet traffic, as well as systems for efficient processing and analysis of a large amount of data. The equipment sold by Trovicor has been labelled in the past as a tool that was used by certain governments to commit massive human rights abuses, so *Privacy International* filed a lawsuit against the company for selling this equipment to the government of Bahrain, which used it to spy on human rights activists.[14] The dangers of this company's products were pointed out by Reporters Without Borders, who called Trovicor the "enemy of the Internet".[15]

Maltego is a German company that produces a research platform which allows the user – through integrated and purchased databases, such as e.g. Social Links – to start with a blank document and show who is connected to whom, to form links, graphs and maps, and to track targets' online activities. This platform can map up to one million entities per investigation, i.e. 64,000 entities per given command.[16] Maltego also includes free options, but these allow access to much fewer data than some of the more advanced versions that include purchased databases such as Maltego One or Maltego Enterprise, which are intended for companies and institutions.

Social Links, a module within the Maltego platform, serves to collect and analyse data from the Internet and social networks. Using facial recognition software, these tools can figure out the identity of a person from an image, and find out exactly which people said person is connected to and what the nature of that relationship is. Social Links is believed to also have the ability to hack into private social media correspondence and to find a person's telephone number even when the user hides this sort of information.[17]

Such tools cause a great deal of concern, as information that can be obtained through them is of greater value than those that can be obtained through traditional spying methods such as wiretapping or video surveillance.

Mozenda is an independent programme for automatic extraction of data from web pages, a so-called "web scraper". The programme also has the ability to change the IP address in order to avoid being blocked by the server during unauthorised downloads of textual and visual content as well as documents.[18]

Clearview AI is an American company that produces facial recognition software. They have the largest database in the world of over 30 billion images/photographs downloaded from the Internet, including those from social networks, from which they collect data. Their facial recognition software has 99% accuracy across all categories, including age, gender and race. Because of the intrusiveness of this software, lawsuits have been filed against the company in many countries around the world – including Canada, Australia, France, Italy and the UK – to prevent it from collecting people's data in this way, without their permission. In some cases, the company was only ordered to delete residents' biometric data; Italy and the UK, on the other hand, went a step further and also fined Clearview AI in the amounts ranging from EUR 10 to 20 million. Sweden has fined its own police force for illegally using this software.[19] To date, Clearview AI has been the subject of more than 15 legal and regulatory actions, and the number is increasing with each passing year. After the American Civil Liberties Union (ACLU) sued Clearview AI before an Illinois court for violating the privacy law, the company has been banned from selling its services to most US companies.[20] The danger of misuse of this software is great, and more and more countries are now fighting against its use.

The Social Card System

The system of mass digital surveillance by use of artificial intelligence was introduced in Serbia through the social card programme, which monitors the activity of individuals (by accessing data from state records) and their contacts with other people. This serves to calculate possible income and thus determine whether someone is eligible for welfare assistance or not. The entire process is automated, so an individual who does not completely fit into the parameters that have been set falls out of the social protection system. This system particularly affects members of the Roma community, whose minimal additional income from the sale of secondary raw materials is sufficient for the algorithm to delete them from the list. Since the beginning of the application of this technology, more than 22,000 citizens of Serbia have lost welfare assistance.[21]

In addition to discrimination, the fact that the system continuously collects enormous amounts of data on citizens, thus endangering their right to privacy, is another big problem. The social card system collects more than 130 pieces of data about welfare beneficiaries and their relatives, using an algorithm whose mode of functioning is not

known to the public. Information about it is kept hidden under the pretext of protecting national security. The fact that the system lacks an adequate form of protection and control is interesting as well, since an adequate risk assessment was not made at the time of its creation. Also, the Law on Social Cards does not contain the definition of special measures that would prevent the export of data and sharing them with third parties.[22] A similar system was active for several years in the Netherlands, but it was banned by the decision of the District Court in The Hague in early 2020 precisely because of its shortcomings, which are now present in Serbia. All in all, the existing social card system is a tool for systematic discrimination of vulnerable groups and denial of social assistance under the veil of the "objectivity" of the algorithm, and another form of mass control of citizens who, in order to receive the necessary welfare assistance, are forced to give up their right to privacy.

The Data Centre in Kragujevac

Since 2020, the information on Serbian citizens and institutions have been kept in the State Data Centre in Kragujevac. Another facility was opened in 2022 to store data from the army, the police and the Security Information Agency. It also includes the first state artificial intelligence platform.[23] With the help of the World Bank, Serbia has invested EUR 55 million in the entire project, and it is believed that the data is very well protected from both physical and cyber attacks.[24] The government established the company named Data Cloud Technology d.o.o, which is fully owned by the state and performing commercial activities.[25] The State Data Centre will also encompass a regional data storage center of the Chinese company "Huawei" for southern and southeastern Europe. The People's Republic of China has donated to the data centre the same company's equipment worth EUR 2 million.[26]

However, although this initiative has the support of experts and international organisations, the fact that the State Data Centre is located in the fenced courtyard of the facility of the Security Information Agency department in Kragujevac can be problematic. Danilo Savić, Director of the company Data Cloud Technology d.o.o. Kragujevac, said that a proper location was very difficult to find, and that they did not even think about this problem. He also added that members of the Security Information Agency department in Kragujevac will not have access to the facilities that store citizens' data, and that they will have to gain access to said data some other way.[27] Considering the many cases when employees of the Security Information Agency and the police, as well as other state authorities, have provided sensitive information to individuals in the media and from political parties, this claim is difficult to believe. The concentration of data in one place does facilitate their protection, but it also makes it easier to use for various purposes, including for the surveillance and control of citizens, as evidenced by digital autocracies such as China.

Name of technology	Type of technology	Description of technology	Type of surveillance	Institutions using the technology	Status of technology
IPC6625-Z30	Smart cameras	They perform video surveillance, have smart video analysis capabilities (identification of objects, recognition of target colours and vehicles). They have a 30x optical zoom and an infrared lamp that reaches up to 150m.	Mass surveillance	MoI (2020)	Active
IPC6225-VRZ-ES	Smart cameras	They perform video surveillance, have smart video analysis capabilities (identification of objects, recognition of target colours and vehicles). They have an optical zoom and an infrared lamp that reaches up to 80m.	Mass surveillance	MoI (2020)	Active
VCN3020	Analysis system	Displays data from smart cameras in real time, has video playback capability and advanced analysis (biometric surveillance for facial recognition and human behaviour analysis).	Mass surveillance	MoI (2020)	Active
Griffeye Analyze	Analysis system	Software for facial recognition and video analysis, which compares the collected data and connects it with other data available on the Internet.	Targeted surveillance	MoI (2021)	Active
Cognyte	Data analysis system	Merges, analyses and visualises a large number of different data sets in order to find information and define patterns of behaviour.	Targeted surveillance	Ministry of Trade, Tourism and Telecommunications (2021)	Active
Maltego	Internet research system	Allows the user to create, by reasearching data bases, a visual representation of who the victim is connected to, create maps and charts, as well as monitor the targets' online activities. The platform can map up to one million entities per investigation.	Targeted surveillance	MoI, Market Inspection, Tax Administration	Active

Name of technology	Type of technology	Description of technology	Type of surveil-lance	Institutions using the technology	Status of technology
Social Links	System for searching for data on the Internet	Serves to collect and analyse data from the Internet and social networks. Using facial recognition software, it can find the identity of the person in a photograph and the exact people said person is connected to as well as the nature of their relationship. It is believed to be able to penetrate private correspondence and access information that is not visible to other users.	Targeted surveil-lance	Market Inspection, Tax Adminis-tration	Active
Mozenda	System for searching for data on the Internet	Serves to automatically extract data from Inter-net pages, i.e. for the so-called "web scraping"	Targeted surveil-lance	Market Inspection	Active
Clearview AI	Analysis system	Serves for facial recogni-tion and has the largest database in the world of more than 30 billion images/photographs downloaded from the Internet, including those from social networks, from which it collects data.	Targeted surveil-lance	MoI (2020)	?
Circles	Spyware	Exploits the weakne-sses of mobile systems to track calls, messages and telephone locations without the need to hack the device itself.	Targeted surveil-lance	BIA (2015) - test	?
Cyberbit Solutions	Spyware	Used for hacking and spying on computers by sending a video link to the victim via email. Once the link is activated, the spyware is installed without the victim's knowledge. It collects all data from the device.	Targeted surveil-lance	Products were presented in Serbia	?

Name of technology	Type of technology	Description of technology	Type of surveil-lance	Institutions using the technology	Status of technology
Trovicor	Spyware	Serves for legal interception by specialised monitoring centres that can intercept telephone calls, SMS messages and all Internet traffic. It also has systems for efficient processing and analysis of a large amount of data.	Targeted surveil-lance	Police Service for Combating Organised Crime (2010)	?
Hacking Team	Spyware	Used for remote hacking and collecting data from hacked devices.	Targeted surveil-lance	BIA, Ministry of Defence (2012)	?
Fin Spy	Spyware	Exploits security flaws in software updates to "attack" the target device. Once installed, the programme collects all data, intercepts calls and tracks the victim's location.	Targeted surveil-lance	BIA (2015)	X
Predator	Spyware	Used to hack the victim's phone, following which it has access to all information on the device such as messages, images and saved passwords. It also gains access to the camera and microphone, through which it spies on the victim and tracks his/her calls.	Targeted surveil-lance	Use in Serbia has been discovered	?
Pegasus	Spy software	Contains the most advanced technology of its kind that allows the user to hack someone's telephone remotely, without the victim noticing. Pegasus can access the camera and microphone, as well as all data on the telephone, including messages, calls and e-mails. The software does not require the victim to click on a suspicious link, but rather infects the system without any interaction.	Targeted surveil-lance	Use in Serbia has been discovered	?

Table 1 - Presentation of digital technologies whose testing and use were discovered in Serbia

Inefficiency of Digital Surveillance

Governments around the world justify the introduction of biometric surveillance and spyware by arguing that such technologies significantly contribute to the fight against various forms of crime. However, this argument is in fact used to make the population accept the introduction of new mechanisms of (digital) control more easily, in fear for their own security. The situation is the same in Serbia. However, it is necessary to primarily determine whether these technologies are really that useful in detecting and preventing crime, considering that the evaluation of their effectiveness has so far been based more on trust than on any real achievements.

Research shows that these technologies, especially mass biometric surveillance, in addition to the fact thet they endanger the privacy of the population, are not effective in preventing crime and terrorism. First of all, mass surveillance systems scan the environment every second and collect an enormous amount of various data, often making it difficult for inspectors to distinguish, in this sea of information, things that are important from those that are. Analysis of terrorist attacks around the world has shown that mass surveillance is not effective in preventing violent crime, and that these cases were solved using classic investigative methods and human intelligence. The US National Intelligence Agency did have mass surveillance at the Boston Marathon in 2013, but two brothers still managed to quietly plant and detonate two bombs near the finish line, killing three people. Even during the pursuit of the perpetrators, relevant information came from foreign governments and from reviewing photographs and videos that were taken by private individuals. Also, the brothers were on the watch list - TIDE, but despite the fact that the US intelligence agency was monitoring their communications, it failed to discover their plan to commit a terrorist act.[28]

The case of Robert Julian-Borczak Williams, who was wrongly arrested by the Detroit police in 2020 on suspicion of committing property theft, is quite illustrative. The main piece of evidence against him was a video surveillance photo that was run through facial recognition software, which identified Williams as the perpetrator. However, after arresting and questioning the suspect, police discovered that the software had incorrectly identified Williams.[29] We can note two problems in this case. The first is that facial recognition systems can make mistakes, especially with people of different races, since the system is most accurate when it comes to white men. The second problem is that the police relied only on information that was provided by the technology, and not on traditional investigative methods.

Speaking about Serbia, one of the famous cases where advanced technologies were insufficient to find the perpetrators of a crime was the murder of one of the leaders of the Kosovo Serbs, Oliver Ivanović, in 2018. Despite numerous cameras that were installed near the crime scene, no recordings that could be used to find the perpetrator have been found to date. The fact that members of the Serbian police and security services were responsible for that area is interesting as well.[30] Despite all these available tools, this case remained unsolved.

Abuse of Digital Surveillance Technologies

The greatest danger of implementing mass biometric surveillance and analysis systems, as well as spyware, is the high level of possibility of their misuse, especially when some of these technologies are almost impossible to detect, as is the case with Israeli Pegaz or Predator spyware. State institutions most often abuse these technologies by using them to monitor political opponents, activists and journalists. These abuses are very important in countries with semi-democratic and non-democratic systems, because they can endanger the freedom and lives of political opponents of the government. For example, cases of misuse of biometric surveillance are quite common in Russia, where their number significantly increased after the invasion of Ukraine. These technologies are used to identify persons who participate in protests against the government, while lately the most frequent targets have been activists who participate in anti-war protests and journalists who write articles that are ctitical of the Putin regime. Once these people are recorded and identified by one of more than 3,000 biometric cameras, their participation in protests is often punished by detention, extended detention or arrest. The situation with the abuse of these technologies is deteriorating, and the Russian police have recently started to preemptively detain activists and journalists immediately prior to certain important events, or when large anti-war protests are planned. A Reuters investigation found that biometric surveillance played a significant role in the arrest of several hundred political dissidents.[31]

Cases of abuse can be found even in democracies with good legal systems and long rule of law traditions. In the United States, for example, the New York police have admitted to using facial recognition software to identify activists who participated in the Black Lives Matter protests which erupted after police officers killed George Floyd in 2020. In one case, police showed up at the door of David Ingram, a 28-year-old activist and protester who was identified by the facial recognition software. The police claimed that the software was only used on footage that was taken from street cameras, but witnesses who gathered outside Ingram's home claimed that the police were also using footage from social media, exceeding NYPD restrictions. The New York Police Department has been using Clearview AI since 2011, so it is very likely that it was precisely this facial recognition software that was used in Ingram's case.[32] Austria, whose police used a biometric surveillance system to identify protesters, was not immune from such abuses either.[33]

Serbia

Serbia is another country that is not immune from this type of abuse, so illegal tracking and wiretapping has become a daily routine against opposition politicians, activists and journalists. Unlawfully collected information often ends up in the hands of representatives of ruling parties or editors of pro-government media. The so-called "VulinGate" affair,[34] from the beginning of 2020, irrefutably proved this practice. Namely, speaking for the *Tanjug* agency, Minister of Defence Aleksandar Vulin harshly criticised the text Dragan Šutanovac, former Minister of Defence and currently member of an opposition party, wrote for magazine *Nedeljnik*. However, the text itself had not yet been published, and had existed only in the form of email correspondence between Šutanovac and Veljko

Lalić, the editor-in-chief of *Nedeljnik*. It is believed that Vulin could have gained access to these data only if Šutanovac or Lalić, or both, had been under surveillance and the security services had intercepted their correspondence. The Ministry claimed that the error had occurred in their PR service, and that they meant the text of the tabloid *Kurir*, not *Nedeljnik*. The case was decided upon by the Committee for the Control of Security Services, which, after an extraordinary control of the Military Security Agency, unanimously decided that the MSA had not applied any special procedures and measures that could collect data from the above persons' communication. It is also important to note that there was not a single opposition politician in the Committee for the Control of Security Services at that time, as well as the fact that the international media organisation Reporters without Borders publicly called on the authorities to further investigate this event.[35]

Two more similar cases of abuse of special measures and procedures took place in May 2023 alone - the first at the beginning of May, when the editor-in-chief of tabloid *Informer* exclusively revealed during his guest appearance on "Pink" television that the editor of the Crime and Corruption Research Network (KRIK), Stevan Dojčinović, had spent five months preparing – in cooperation with the American media organisation "The New York Times" – a text in which Veljko Belivuk's clan would be connected with the state, and that the text will be published the next day. Shortly afterwards, Dojčinović replied on Twitter that the information was in fact correct, but wondered how the editor of *Informer* received it and whether it was once again a matter of "collaboration" with the security services.[36]

In the middle of May, *Informer* published an article in which, once again, it exclusively revealed that the British newspaper "The Guardian" will be publishing a text criticising the government of President Aleksandar Vučić, and that their interlocutors will be "haters of Serbia from the NGOs", that is, representatives of the Belgrade Centre for Security Policy (BCSP) and the Bureau for Social Research (BIRODI). The question here is where *Informer* got this information three days before the publication of the article, and whether this was another case of illegal wiretapping of journalists and researchers.[37]

The same happened during the "Serbia against Violence" protests in May, when activists wondered if the government was wiretapping them. Namely, President Vučić announced that activists would block the Gazela Bridge during the protest, although this information was not known to the public as it was discussed only the day before, at the protest headquarters.[38] The event from 2021, when one of many environmental protests was held in Novi Sad, also indicated that activists were indeed subjected to digital surveillance. Members of the ecological movement *Eko Straža* noticed that some participants were filming them with their telephones, using special facial recognition software. Their fear was somewhat confirmed by the fact that some citizens received misdemeanor warrants for participating in the road blockade at their home addresses, although no one at the protest had asked them for any form of ID. The law allows members of the police to record public gatherings with prior notice, but the use of biometric surveillance does not fall under their jurisdiction and seriously violates citizens' privacy. This case of misuse of biometric surveillance against political opponents remained unexplained.

Competences and Powers of State Institutions regarding Digital Surveillance

State institutions in Serbia acquired digital programmes and technologies for citizen surveillance, but this was not accompanied by a change in the legal framework. The question thus arises about the legality of the use of these softwares and tools, that is, whether the institutions are competent and authorised to apply them. For that reason, in the following part of the report we will present the competences and powers of the state institutions of Serbia that procured digital technologies for the surveillance of citizens.

Security Information Agency (BIA)

Compared to other regulations that govern the work of state institutions that procured digital surveillance technologies, the Law on the Security Information Agency contains the most precise provisions that regulate their competences and powers. As stated in Article 9, "While operating within its jurisdiction, the Agency shall apply adequate operational methods, measures and activities, as well as appropriate operational and technical means to collect data and information." The Law defines when special measures can be used, who approves them and how long they last. Special measures include secret surveillance and recording of communications, *regardless of the form and technical means used for it, or surveillance* of electronic or any other address, secret surveillance and recording of communications in public places and places with limited access or in premises, statistical electronic surveillance of communications and information systems aimed at obtaining data on communication or location of used mobile terminal equipment, *computer search of already processed personal and other data and their comparing with data acquired through the application of measures*, and secret surveillance and recording of locations, premises and objects, including devices for automatic data processing and equipment used or potentially used for storing electronic records (Law on BIA, Article 13). However, the Law does not mention the possibility of using biometric surveillance and data processing.

Although the Law on the Security Information Agency formulates the definitions concerning jurisdiction and authority more precisely than other similar laws do, they are still not sufficiently clear. The first problem can be found in Article 2, where the field of action is defined very broadly, referring to the protection of the security of the Republic of Serbia and the constitutional order. This definition, without further specification, gives members of the Agency a free hand to broadly interpret what constitutes national security, which creates room for abuse. Another omission is the absence of provisions on the collection and processing of data using biometric technologies and digital surveillance tools.

Military Security Agency (MSA)

Similarly to the Law on the Security Information Agency, the Law on the Military Security Agency regulates tasks and competencies somewhat more precisely than other laws do. Within the security protection of the Ministry of Defence and the Serbian Armed Forces, the MSA, among other things, detects, investigates and documents certain criminal acts and collects, analyses, processes and evaluates counterintelligence data within its purview (Law on the Military Security Agency and the Military Intelligence Agency, Article 6). The MSA is authorised to collect data by means of special procedures and measures when it is not possible to collect data otherwise or when their collection involves excessive risk to life and health of people and property, i.e. excessive costs (Law on the Military Security Agency and the Military Intelligence Agency, Article 11). Article 12 specifies special procedures and measures of covert data collection within the competences of the MSA that involve the use of "technical means". However, further text of the Law does not define what these technical means are, and some provisions are still defined too broadly.

Police

The Law on Police contains highly *general provisions* on the protection of citizens and the detection and investigation of criminal acts, and does not mention the use of these and similar technologies (Law on Police, Article 30). The provisions contained in the Criminal Procedure Code are somewhat more detailed. Evidentiary actions against persons include checking accounts and suspicious transactions based on information provided by banks and other financial institutions (Criminal Procedure Code, Article 143). The police, BIA and MSA are authorised to perform special evidentiary actions such as covert communication surveillance and covert tracking (Criminal Procedure Code, Articles 166-173). Computer searches of data are carried out by the police, BIA, MSA, as well as customs, tax or other services or other state authorities that exercise public powers based on the law (Criminal Procedure Code, articles 178-180).

Tax Administration

The Tax Administration is authorised, among other things, to collect evidence in tax proceedings by various means, including "any other means of establishing facts" (Law on Tax Procedure and Tax Administration, Article 43). The Tax Administration further provides tax services, carries out tax control and carries out activities aimed at detecting tax crimes (tax police). The tax police act as an internal affairs authority and are authorised to take *all required actions, in accordance with the law, with the exception of movement restriction* (Law on Tax Procedure and Tax Administration, Article 135). Devoid of further clarification, this definition leaves room for the misuse of biometric technology

Market Inspection

The Law on Inspection Supervision defines the Inspection as a body that operates within the composition, an internal organisational unit, or as inspectors of a state administration body, i.e. a body of the autonomous province, a local self-government unit or other entity with public powers that performs inspection supervision (Law on Inspection Supervision, Article 3). The Inspection collects data and monitors and analyses the situation in the field of inspection supervision within its purview. Its tasks include the collection and analysis of data obtained by means of checklists, conducting surveys and public opinion research and *other direct data collection* (Law on Inspection Supervision, Article 8), which is a rather broad definition.

Market Inspection and market inspectors are governed by the Law on Trade, but that Law does not state that the market inspection is allowed to use sophisticated biometric technologies. The powers of a market inspector are defined quite broadly and include, among other things, photographing, video recording of the area in which supervision is carried out, i.e. goods and other items that are the subject of supervision, collecting data relevant to the subject of supervision, and requesting assistance from the police or municipal police (Law on Trade, Article 48). As regards securing evidence, the Law only states that a market inspector can temporarily confiscate certain items (Law on Trade, Article 64).

***

After presenting the competences and powers of the state authorities which have used, are using and/or have expressed interest in using spyware, biometric surveillance and other intrusive technologies, it is clear that their competences and powers are defined quite broadly. Even when special measures are described in greater detail, as in the Law on the Security Information Agency, the purpose of their use is defined too broadly: it includes the protection of security and the constitutional order of the Republic of Serbia, as well as research, collection, processing and evaluation of data without further clarification as to the manner and tools envisaged for these activities. There are therefore no provisions that clearly indicate that BIA or MSA can use biometric data processing and digital surveillance technologies. Insufficiently clear statutory provisions leave room for abuse and for exceeding the powers of these authorities. Technology is developing very quickly, while the laws remain the same. Due to the emergence of more and more intrusive and accessible technologies, it is necessary to amend the laws and specify the provisions in them so as to make the legal system more applicable to the current situation in the country and the EU, which Serbia aspires to join.

How Biometric Surveillance is Regulated in the EU

Membership in the European Union (EU) is (still) Serbia's priority, and in this respect Serbia has an obligation to align its legal framework with the EU *acquis*. That is why it is important to know how the EU has regulated the field of biometric surveillance and data processing, that is, how it will regulate it in the coming period and to what extent Serbia deviates therefrom. In the following section of the report, we will provide a brief overview and analysis of this area in the EU.

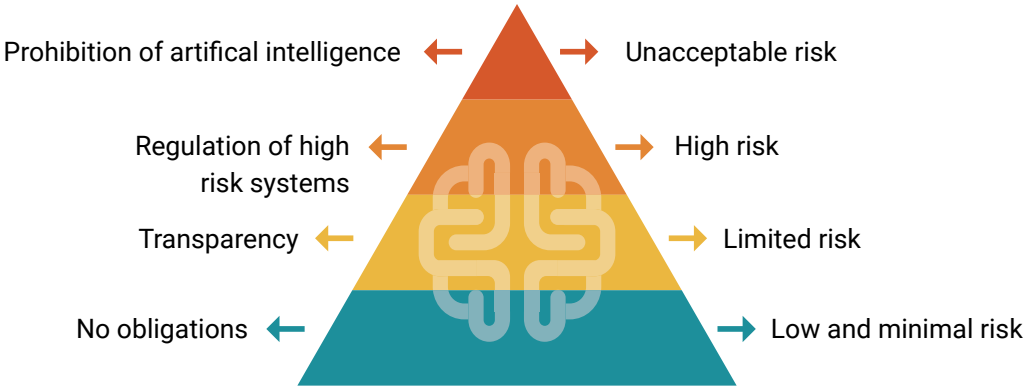
The European Union regulates the field of biometric surveillance in several different documents, the most important of which are the EU Charter of Fundamental Rights (CFR), the EU General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED). In addition, there was an initiative to unify the legislation in this field in a special Bill on Artificial Intelligence, which was approved by a large majority in the European Parliament in mid-June. The future of the bill will be further decided during the so-called "trialogues", i.e. negotiations between the European Parliament, the European Commission and the Council of Ministers.

The Charter regulates the areas of privacy rights and data protection rights, as well as the area dealing with the fight against discrimination. According to the provisions of the GDPR and LED, the processing of facial images must be carried out in accordance with the law and the principle of proportionality, and must also be transparent and fair, i.e. non-discriminatory. In addition, the data may be analysed only for specific, explicit and legitimate purposes, which means that the intended purpose must be formulated precisely enough so that the person whose data is being processed can foresee the purpose for which said data will be processed. In this case too, the principle of proportionality and data protection, as well as other conditions such as reasonable suspicion and limited search, must be met.

In 2020, the European Commission published a White Paper on artificial intelligence proposing to define specific situations in which biometric surveillance would be allowed. The EU's high-level expert group on artificial intelligence called for a clearer definition of artificial intelligence itself, as well as for a clearer definition of when and how it can be used, to distinguish between identifying and finding/tracking people, and between targeted and mass surveillance. The European Parliament has called for restrictions on facial recognition software on several occasions, first in the form of a complete moratorium on the use of facial recognition systems in public places by public authorities, in health and educational institutions, as well as a moratorium on the use of these systems by the police.

In 2021, the European Commission published a draft Artificial Intelligence Act concerning the use of artificial intelligence and the risks arising therefrom. This document mandates the prohibition of particularly harmful artificial intelligence practices that are contrary to the values of the Union, which manipulate human behavior through the use

of subliminal communication techniques and social scoring systems and social cards. It also classifies artificial intelligence systems by level of risk into unacceptable, high, limited, and low or minimal risk systems. Unacceptable risk systems are to be completely prohibited, while high risk systems would require regulation. Limited risk systems would be subject to transparency, while no obligations would be set for low or minimal risk systems. The European Parliament adopted this act on 14 June 2023.



The AI Act will classify different artificial intelligence systems based on risk levels
Image: European Commission

Diagram 1. The Draft of Artificial Intelligence Act and treatmant of different types of risks

The proposal contains stricter classification criteria for artificial intelligence tools, based on which a number of applications will be prohibited for use in the EU, such as:

- Real-time biometric identification systems in public spaces,
- Biometric systems of categorisation according to personal characteristics such as gender, racial and ethnic affiliation, religious and political orientation,
- Predictive police systems based on profiling,
- Systems for recognising emotional states, i.e. their use by the police, at border crossings, in the workplace and in educational institutions,
- Automated collection of biometric data from social networks or security camera footage.

Biometric identification is allowed only and exclusively in cases of serious criminal investigations, provided that there is an approval by the court.[39] The law should regulate systems for generating content, predictions, recommendations or decisions that affect environments - including tools for interacting with people, such as ChatGPT, smart surveillance systems or applications that can be used to generate the so-called deepfake content.[40]

The future of the law will be discussed by the European Parliament, the European Commission and the Council of Ministers during a "trialogue", where the positions of member states who believe that such systems are useful in the fight against crime, and human rights experts who believe that biometric surveillance does not automatically bring greater security, will come face to face with their arguments. If approved, the law will likely come into effect no earlier than in 2025.[41] As one of the first to regulate the matter, it will have a major impact on legal systems around the world in the field of artificial intelligence.

This act is significant for the future of the regulation of artificial intelligence in Serbia as well, especially in light of the proposed solutions contained in the Draft Law on Internal Affairs, whose intention was to legalise the application of biometric surveillance. If EU adopts acts on artificial intelligence, the mass use of biometric surveillance in Serbia will be in conflict with the EU *acquis,* with which Serbia is aligning its legislation in order to fulfill a membership requirement.

Sources and Notes

Sources and Notes

1 Marko Crnjanski, "There are more and more Huawei cameras in the streets of Belgrade – What is their purpose and can they recognise your face?", *Netokracija,* 17 June 2020, https://www.netokracija.rs/huawei-kamere-beograd-171048

2 *Ibid.*

3 Dana Priest, Craig Timberg and Souad Mekhennet, "Private Israeli spyware used to hack cellphones of journalists, activists worldwide", *The Washington Post*, 18 July 2021, https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

4 "Greece passes intelligence bill banning the sale of spyware", *The Guardian*, 9 December 2022, https://www.theguardian.com/world/2022/dec/09/greece-passes-intelligence-bill-banning-the-sale-of-spyware

5 Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert, "Running in Circles, Uncovering the Clients of Cyberespionage Firm Circles", *Citizen Lab,* 1 December 2020, https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

6 Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert, "Champing at the Cyberbit, Ethiopian Dissidents Targeted with New Commercial Spyware", *Citizen Lab,* 6 December 2017, https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/#:~:text=This%20report%20describes%20how%20Ethiopian,PhD%20student%2C%20and%20a%20lawyer

7 Aleksa Tešić, "Israeli spyware: Citizens of Serbia targeted by Predator", *Birn*, 3 March 2022, https://birn.rs/izraelski-softveri-za-spijunazu-gradani-srbije-na-meti-predatora/

8 Moira Lavelle, "Reporters dig up more links between Greek government and spyware", *Al Jazeera,* 17 November 2022, https://www.aljazeera.com/news/2022/11/17/reporters-dig-up-more-links-between-greek-government-and-spyware

9 "Munich-based tech company Fin Fisher dissolves after investigations", *ECCHR,* https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfisher/

10 *Ibid.*

11 Sing, Evie Kim, "Israel's Cognyte embroiled in Myanmar in spyware scandal", *Identity week,* 16 January 2023, https://identityweek.net/israels-cognyte-embroiled-in-myanmar-in-spyware-scandal/

12 Griffeye, accesed on 5 June 2023, https://www.griffeye.com

13 Lorenzo Franceschi-Bicchierai, "Hacking Team Founder: Hacking Team is Dead", *VICE,* 26 May 2020, https://www.vice.com/en/article/n7wbnd/hacking-team-is-dead

14 Privacy International *et al*. v. Trovicor, *OECD*, accessed on 5 June 2023, https://www.oecdwatch.org/complaint/privacy-international-et-al-vs-trovicor/

15 "Import and use of surveillance equipment in Serbia: The Trovicor case", *Share foundation,* 28 November 2013, https://resursi.sharefoundation.info/sr/resource/uvoz-i-upotreba-opreme-za-nadzor-u-srbiji-slucaj-trovicor/

16 Aleksa Tešić, "Software for processing personal data is a potential threat to citizens' privacy", *Birn*, 3 June 2022, https://birn.rs/softveri-za-obradu-licnih-podataka-potencijalna-pretnja-po-privatnost-gradana/

17 *Ibid.*

18 *Ibid.*

19 "About Clearview AI's mockery of human rights, those fighting it, and the need for EU to intervene", *Reclaim your face,* 28 March 2022, https://reclaimyourface.eu/about-clearviewai-mockery-human-rights-those-fighting-eu-interveen/

20 James Clayton and Ben Derico, "Clearview AI used nearly 1m times by US police, it tells the BBC", *BBC,* 27 March 2023, https://www.bbc.com/news/technology-65057011

21 Natalija Jovanović and Dušan Komarčević, "Digitalisation of poverty in Serbia: Deprived of assistance because they sell secondary raw materials", *Radio Free Europe,* 29 November 2022, https://www.slobodnaevropa.org/a/srbija-socijalne-karte-algoritam/32153869.html

22 *Ibid.*

23 "The second building of the State Data Centre in Kragujevac has been opened", *RTS,* 7 July 2022, https://www.rts.rs/lat/vesti/drustvo/4877424/otvoren-drugi-objekat-drzavnog-data-centra-u-kragujevcu.html

24 Marko Crnjanski, "Exclusive: We visited the 14.000m² State data centre in Kragujevac – One of the most modern in this part of Europe ", *Netokracija,* 4 February 2021, https://www.netokracija.rs/data-centar-kragujevac-180295

25 Marijana Avakumović, "American and Chinese companies are storing data in Kragujevac", *Politika*, 5 March 2022, https://www.politika.rs/scc/clanak/501173/Americke-i-kineske-kompanije-cuvaju-podatke-u-Kragujevcu

26 Brane Kartalović, "Data centre BIA's courtyard", *Politika*, 30 October 2019, https://www.politika.rs/scc/clanak/440891/Data-centar-u-dvoristu-BIA

27 *Ibid.*

28 Jennifer Stisa Granick, "Mass spying isn't just intrusive - It's ineffective", *Wired,* 2 March 2017, https://www.wired.com/2017/03/mass-spying-isnt-just-intrusive-ineffective/

29 Kashmir Hill, "Wrongfully accused by an algorithm", *The New York Times*, 24 June 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

30 Slobodan Maričić, "Kosovo and Oliver Ivanović, four years later: When will the murder of one of the leaders of Kosovo Serbs be solved?", *BBC*, 16 January 2022, https://www.bbc.com/serbian/lat/srbija-59998523

31 Lena Masri, "Facial recognition is helping Putin curb dissent with the aid of U.S. tech", *Reuters,* 28 March 2023, https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/

32 JamesVincent, "NYPD used facial recognition to track down Black Lives Matter activist", *The Verge*, 18 August 2020, https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram

33 Andreea Belu, "Evidence: Biometric mass surveillance in EU", *LinkedIn*, 6 April 2021, https://www.linkedin.com/pulse/evidence-biometric-mass-surveillance-eu-andreea-belu/

34 "The 'VulinGate' affair: How did the Minister manage to read the text which was never published in Nedeljnik?", *Nedeljnik*, 2 February 2020, https://www.nedeljnik.rs/afera-vulingejt-kako-je-ministar-procitao-neobjavljeni-tekst-u-nedeljniku-citajte-u-novom-broju/

35 "National Assembly of Serbia: MSA did not intercept communication between Šutanovac and the editor of Nedeljnik magazine", *Radio Free Europe*, 21 February 2020, https://www.slobodnaevropa.org/a/30447609.html

36 "Stevan Dojčinović: The story of Belivuku and those in power really is to be published tomorrow in the New York Times, but how does Vučićević know that?", *Danas*, 2 May 2023, https://www.danas.rs/vesti/politika/stevan-dojcinovic-prica-o-belivuku-i-vlastima-izlati-sutra-u-njujork-tajmsu-ali-odakle-to-vucicevic-zna/

37 "Informer reveals Guardian's interlocutors in the text about Vučić four days in advance", *N1*, 16 May 2023, https://n1info.rs/vesti/informer-cetiri-dana-ranije-otkrio-ko-su-sagovornici-gardijana-u-tekstu-o-vucicu/

38 *Ibid.*

39 "In anticipation of the European Law on AI: Wide prohibition of biometrics and predictive police systems", *Share Foundation*, 26 May 2023, https://www.sharefoundation.info/sr/cekaju-ci-evropski-zakon-o-ai-siroka-zabrana-biometrije-i-prediktivnih-policijskih-sistema/

40 *Ibid.*

41 Masha Borak, "EU Parliament approves AI Act amid heated biometrics debates", *Biometric update*, 4 June 2023, https://www.biometricupdate.com/202306/eu-parliament-approves-ai-act-amid-heated-biometrics-debates

BCSP Belgrade Centre for Security Policy

bezbednost.org